GUIDE ANIMATEUR

Sécurité numérique

Usage exclusif de l'équipe d'animation

2 heures
4 à 8 participants

OBJECTIFS PEDAGOGIQUES

- Créer et mémoriser un mot de passe solide
- Reconnaitre les tentatives d'arnaque courantes
- Activer le verrouillage du téléphone
- Identifier un site sécurisé (HTTPS, cadenas)
- Savoir quelles informations ne jamais communiquer

SEQUENCE PEDAGOGIQUE DETAILLEE

#	Phase	Actions de l'animateur	Variante / Conseil
1	**Accueil et parole** *15 min*	Question ouverte : 'Avez-vous déjà reçu un message suspect ou un faux appel ?' Laisser les participants témoigner. Déprivatiser : 'C'est très courant, on va apprendre à se protéger ensemble.'	*Si aucun témoignage : raconter un exemple concret et connu (type arnaque au colis)*
2	**Mots de passe** *25 min*	Montrer un mot de passe faible vs fort. Expliquer la méthode phrase-code : 3 mots du quotidien + chiffre + symbole. Exercice papier : chaque participant crée son propre mot de passe. Rappeler : ne pas l'écrire sur un post-it colle à l'écran !	*Aborder les gestionnaires de mots de passe pour les participants avance*
3	**Arnaques et phishing** *20 min*	Projeter 3 exemples réels (email, SMS, appel). Pour chaque exemple : demander 'C'est vrai ou faux ?' Expliquer les 5 signes d'alerte. Insister : une banque ou un organisme officiel ne demandera JAMAIS de mot de passe par téléphone.	*Adapter les exemples au profil : SMS colis pour les acheteurs, faux EDF pour les autres*
4	**Connexion sécurisée** *15 min*	Montrer le cadenas HTTPS dans le navigateur. Comparer deux URLs (vraie vs fausse). Exercice : trouver le cadenas sur ameli.fr et impots.gouv.fr.	*Préciser que le cadenas garantit le chiffrement mais pas l'honnêteté du site*
5	**Sécuriser le téléphone** *20 min*	Vérifier avec chaque participant si leur téléphone a un code de verrouillage. Accompagner l'activation si absent. Mentionner les mises à jour automatiques et leur utilité.	*Eviter de voir les codes personnels : guider sans regarder*
6	**Ce qu'on ne partage jamais**	Liste conjointe avec les participants : code bancaire, numéro sécu, mot de	*Aborder les arnaques 'au sentiment' (faux*

	15 min	passe, scan de carte d'identité... Afficher la liste finale et la faire coller sur la fiche usager.	*petits-enfants en danger) si le public est senior*
7	**Bilan** *10 min*	Recapituler les 5 reflexes essentiels. Distribuer la fiche usager. Questions.	*Proposer une permanence pour les cas personnels déjà vécus*

POINTS DE VIGILANCE SPECIFIQUES

POSTURE BIENVEILLANTE ET NON-CULPABILISANTE

Certains participants ont peut-être déjà été victimes d'arnaques financières : ne pas insister, respecter la pudeur

Ne jamais regarder ni noter les mots de passe ou codes personnels des participants

Si un participant signale une arnaque en cours : l'aider à contacter sa banque ou le 17, ne pas gérer seul

Rappeler que les arnaques ciblent tout le monde, y compris les personnes très instruites

GESTES PEDAGOGIQUES RECOMMANDES

Utiliser des vrais exemples imprimés plutôt qu'une description orale – l'impact visuel est plus fort

Faire repérer les signes d'arnaque par les participants eux-mêmes avant de donner la réponse

La méthode phrase-code : la faire pratiquer sur papier, pas directement sur l'appareil

Pour la double authentification : expliquer le principe sans l'imposer – certains n'ont pas de second appareil

PREPARATION AVANT LA SEANCE

Matériel	• 3 exemples imprimés d'arnaques réelles (email phishing, SMS colis, faux appel banque) • Feuilles vierges pour l'exercice mot de passe • Fiches usager imprimées (1 par participant) • Exercices pratiques imprimes
Vérifications	• Tester la démonstration HTTPS sur navigateur (ameli.fr, impots.gouv.fr) • Préparer un diaporama avec les exemples d'arnaques projetés • Connaitre la procédure d'activation du verrouillage sur iOS et Android